Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 5174073, 2 pages
https://doi.org/10.1155/2017/5174073

Editorial

Wireless and Mobile Networks: Security and Privacy Issues

Arun Kumar Sangaiah,[1] Marimuthu Karuppiah,[1] and Xiong Li[2]

[1]*School of Computing Science and Engineering, VIT University, Vellore 632014, India*
[2]*Hunan University of Science and Technology, Xiangtan, China*

Correspondence should be addressed to Arun Kumar Sangaiah; arunkumarsangaiah@gmail.com

Received 1 October 2017; Accepted 4 October 2017; Published 1 November 2017

With the advent of 5G networks in the era of Internet of Things (IoT), wireless and mobile networking have become prevalent everywhere. In this scenario, security and privacy have become the decisive factors. Mobile and wireless ecosystem is an ideal playground for countless perpetrators. (i) Handheld devices are often utilized for critical tasks, such as e-commerce, bank transactions, and application purchases as well as social interactions. (ii) These devices uniquely identify their users and store sensitive and meticulous information about them. (iii) Despite their sophistication, naive security mechanisms have culminated in the bypassing of the mobile operating systems. Moreover, several wireless interfaces and protocols have been found to be vulnerable. As the attacker has a multitude of alternate entry points to perform penetration, the inception of assaults against the user and underlying systems had augmented both in amount and in matters of complexity. Therefore, it is imperative to note that novel and advanced security and privacy-preserving measures should be deployed. This special issue has acknowledged overwhelming responses from researchers, and it has received many high-quality submissions from various countries around the world. All the submitted papers have been reviewed by at least three independent experts. We expect that this special issue focuses on cohesive information related to the applications of security and privacy issues in wireless and mobile networks, and it also delivers stimulations for future research.

In the paper entitled "Multiorder Fusion Data Privacy-Preserving Scheme for Wireless Sensor Networks" M. Xie et al. propose multiorder fusion data privacy-preserving (MOFDAP) scheme based on the idea of SMART algorithm. In this paper, the authors have introduced interference code protection and adopt the idea of multiorder fusion to implement a proposed scheme. The simulation results show that the proposed MOFDAP scheme has a better privacy protection function under low traffic.

The paper of L. Wang and Q. Wang entitled "Secure-Network-Coding-Based File Sharing via Device-to-Device Communication" proposes a large scale file sharing scheme based on secure network coding via device-to-device (D2D) communication. In the proposed scheme, when a user needs to share data with others in the same area, the source node and all the intermediate nodes need to perform secure network coding operation before forwarding the received data. The experimental results show that secure network coding is very feasible and suitable for such file sharing. Moreover, the sharing efficiency and security outperform traditional replication-based sharing scheme.

In the paper entitled "The High Security Mechanisms Algorithm of Similarity Metrics for Wireless and Mobile Networking" X. Wang proposes an improved a priori algorithm based on Boolean matrix and deletes the unnecessary rows and columns of the matrix to reduce the scale of the data and apply to agricultural datasets. Experimental results show that the improved a priori algorithm can efficiently discover useful association rules for the reason that database will be scanned for only one time and that the data to deal with is getting smaller and smaller with the algorithm running.

A. Khan et al. present a partial permutation encryption (PPE) algorithm in their paper entitled "Energy Efficient Partial Permutation Encryption on Network Coded MANETs" to propose P-Coding scheme that permuted only Global Encoding Vectors which decrease the computational complexity making it an efficient encryption scheme in terms of energy,

computation, and cost. To authors the security effectiveness of the proposed scheme against various attacks is ensured via proposed dynamic key generation mechanism and random key generation.

In the paper entitled "Security Enrichment in Intrusion Detection System Using Classifier Ensemble" written by U. R. Salunkhe and S. N. Mali, the aim was to enhance detection rate of Intrusion Detection System (IDS) by using machine learning technique. The authors proposed a novel classifier ensemble based IDS using hybrid approach which combines data level and feature level approach. Classifier ensembles combine the opinions of different experts and improve the intrusion detection rate. Experimental results show the improved detection rates of the proposed system compared to state-of-the-art technique.

The paper entitled "Enhancing the Cloud Computing Performance by Labeling the Free Node Services as Ready-To-Execute Tasks," written by R. S. Abujassar and M. Jazzar, introduced a new technique called Cloud Computing Alarm (CCA) mechanism. The proposed CCA is to enhance and increase network service performance by reducing searching time for the node manager by updating the information frequently. In addition, the CCA also improves the Quality of Service (QoS) for sensitive and high priority tasks.

Acknowledgments

We would like to express our sincere gratitude to all the contributors who have submitted their high-quality manuscripts and to the experts for their support in providing review comments and suggestions on time.

Arun Kumar Sangaiah
Marimuthu Karuppiah
Xiong Li